W9827(JP)L Reference 2

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 | A1

(11) International Publication Number: **WO 95/09498**

(43) International Publication Date: 6 April 1995 (06.04.95)

(21) International Application Number: PCT/US94/09519

(22) International Filing Date: 25 August 1994 (25.08.94)

(30) Priority Data:
08/127,718 27 September 1993 (27.09.93) US

(71) Applicant: MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors: FINKELSTEIN, Louis, David; 1698 West Ottowa Court, Wheeling, IL 60090 (US). BROWN, Daniel, Peter; 788 Chatham Avenue, Elmhurst, IL 60126 (US). PUHL, Larry, Charles; 6 Plum Court, Sleepy Hollw, IL 60118 (US).

(74) Agents: PARMELEE, Steven, G. et al.; Motorola Inc., Intellectual Property Dept./ATS, 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

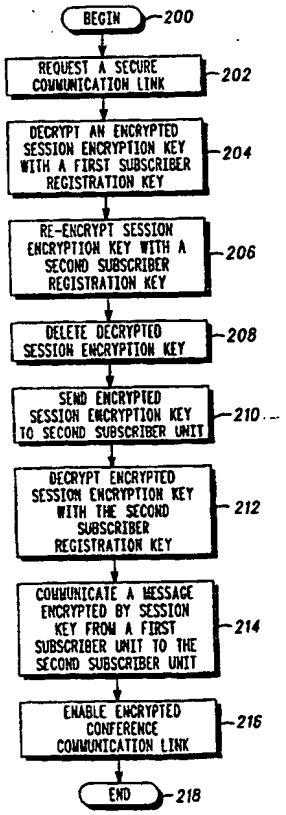
(81) Designated States: FI, JP, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: METHOD FOR KEY MANAGEMENT OF POINT-TO-POINT COMMUNICATIONS

(57) Abstract

A method of secure key distribution in a communication system having a plurality of subscriber units (100, 102) and an infrastructure communication center (104) is provided. A first subscriber unit (100) sends a request (202) to the infrastructure communication center (104) for a secure communication link with a second subscriber unit (102). This request includes an encrypted session encryption key which was encrypted with a first subscriber registration key. The infrastructure communication center decrypts the encrypted session encryption key (204) with the first subscriber registration key. Subsequently, the infrastructure communication center re-encrypts the session encryption key (206) with a second subscriber registration key. This re-encrypted session encryption key is sent (210) to the second subscriber unit.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

METHOD FOR KEY MANAGEMENT OF POINT-TO-POINT COMMUNICATIONS

Related Inventions

The present invention is related to the following invention which is assigned to the assignee of the present invention. Method and Apparatus for Efficient Real-Time Authentication and Encryption in a Communication System by Brown et al. having U.S. Serial No. 08/084,644, and filed on June 28, 1993.

Field of the Invention

The present invention relates to communication systems and, more particularly, to encryption key management of point-to-point communications.

Background of the Invention

Many communications systems currently use encryption to enhance security of the systems. These communication systems include cellular radio telephone communication system, personal communication systems, paging systems, as well as wireline and wireless data networks. By way of example a cellular communication system will be described below; however, it will be appreciated by those

skilled in the art that the encryption techniques described can be readily extended to other communication systems without departing from the scope and spirit of the present invention. Turning now to cellular communication systems, these systems typically include subscriber units (such as mobile or portable units) which communicate with a fixed network communication unit via radio frequency (RF) communication links. A typical cellular communication system includes at least one base station (i.e., communication unit) and a switching center (i.e., an infrastructure communication center). Present cellular communication systems are designed to encrypt communications on an RF link between a subscriber unit and a base station unit through the use of an encryption key known to both units so that others who intercept the RF link communication link will be unable to listen to the communication (e.g., unable to eavesdrop on a voice conversation).

One such RF link encryption technique is described in the United States Digital Cellular (USDC) standard (known as IS-54 and IS-55) and published by the Electronic Industries Association (EIA), 2001 Eye Street, N.W., Washington, D.C. 20006. The USDC system encryption technique utilizes a series of specialized messages which must be passed between the subscriber unit and a base site communication unit before a session encryption key is known to both units. This encryption key is based upon shared secret data (SSD) in USDC system. For an authentication process an SSD_A key is used. Similarly, for a voice privacy function an SSD_B key is used. For the voice privacy function, the initial transmitted subscriber message contains an authentication response, but no other data is encrypted. The command to begin an encryption process is sent from the service provider (i.e., base site communication unit) to the subscriber after the subscriber has been assigned a traffic channel. Further, current system architecture design is focused on bringing encryption to data as well as voice. Data consists of either synchronous or packet data. Ideally, an encryption key should be provided for each data communication session. In a synchronous data environment, a session key is an encryption key which is used for the duration of a single (e.g., circuit switched) data communication (i.e., "call"). Similarly in a data packet environment, a session key is an encryption key which is used from the time that the communication unit registers with a serving system until the next time that the

communication unit re-registers. In addition, in a previously-cited related invention entitled "Method and Apparatus for Efficient Real-Time Authentication and Encryption in a Communication System" by Brown et al. having U.S. Serial No. 08/084,644, and filed on June 28, 1993, another encryption key is proposed for USDC system which is termed an SSD_C key and which is used for data packet encryption. In these communication systems, packetized data also needs to be encrypted. Packetized data adds an additional problem to the typical encryption process. This is because packets of data may arrive at different times at a subscriber unit of a communication unit (i.e., packet messages are "connectionless"). These packets need to be reassembled and decrypted in the same order in which they were encrypted. In addition, an encryption key can only be negotiated when a subscriber performs a registration. Therefore, a need exists for an encryption technique which can alleviate these problems associated with packetized data.

However, these previously known encryption techniques do not address all of the possible eavesdropping vulnerabilities inherent in a communication channel. Eavesdropping may still occur at other points in the communication channel between the subscriber unit and an endpoint target communication device such as through wiretapping of a land-line phone. Such a communication between a subscriber unit and an endpoint target communication device is termed a "point-to-point" communication. The communication may travel along several different physical communication links before being ultimately coupled via a communication link between the subscriber and target devices. For example in the cellular environment, a user of a subscriber unit may place a voice call to a target communication device located at a place of business. In order for that call to be completed, a communication channel must be set up on an RF link to a base site communication unit. In addition, the communication channel must be extended through the public switched telephone network (PSTN) to the place of business. This place of business may have a private telephone network connected to the PSTN. As a result, the communication channel may also need to be extended through the private network to ultimately connect with the target communication device. Currently, encryption techniques are only being applied to individual components of the entire communication channel (e.g., the RF link in USDC system may be encrypted).

However, this leaves other components such as the PSTN or private network vulnerable to eavesdropping through wiretapping. Therefore, a need also exists for an encryption technique which can alleviate these problems associated with eavesdropping at other points of the communication channel.

Summary of the Invention

These needs and others are substantially met through provision of a method of secure key distribution in a communication system having a plurality of subscriber units and an infrastructure communication center. A first subscriber unit sends a request to the infrastructure communication center for a secure communication link with a second subscriber unit. This request includes an encrypted session encryption key which was encrypted with a first subscriber registration key. The infrastructure communication center decrypts the encrypted session encryption key with the first subscriber registration key. Subsequently, the infrastructure communication center re-encrypts the session encryption key with a second subscriber registration key. This re-encrypted session encryption key is sent to the second subscriber unit. In an alternative method, the first subscriber unit and the infrastructure communication center a priori know a session key. Therefore, the infrastructure communication center only needs to encrypt and send the session encryption key to the second subscriber unit, in response to a request by the first subscriber unit.

Brief Description of the Drawings

FIG. 1 is a block diagram showing a preferred embodiment communication system having a first and a second subscriber unit as well as an infrastructure connecting the subscriber units in accordance with the present invention.

FIG. 2 is a flow chart of a preferred embodiment encryption method used by the first and the second subscriber unit over the infrastructure as shown in FIG. 1 in accordance with the present invention.

FIG. **3** is a flow chart of an alternative preferred embodiment encryption method used by the first and the second subscriber unit over the infrastructure as shown in FIG. **1** in accordance with the present invention.

Detailed Description

FIG. **1** generally depicts a first **100** and a second **102** subscriber communication unit (e.g., a radiotelephone) as well as an infrastructure such as an infrastructure communication center or switch **104** and first **106** and second **108** cellular radio base sites. In the following example the subscriber units **100** and **102** are serviced by the same infrastructure switch **104**. The first subscriber unit **100** forms a communication channel with the first base site **106** by an RF link **110**. Similarly, the second subscriber unit **102** forms a communication channel to the second base site **108** by an RF link **112**. In addition, the first base site **106** and the second base site **108** form communication channels to the infrastructure switch **104** by wirelines **114** and **116**, respectively.

However, it will be appreciated by those skilled in the art that multiple switches (e.g., a cellular switch, a local PSTN switch, and/or a long distance carrier switch) could be used to connect the two subscriber units. In addition, the two subscriber units may be a part of two different cellular systems or one connected to a wireline and one a part of a cellular system. Further, the subscriber units could be communicating data rather than voice over a communication channel such as through an Advanced Radio Data Information Service (i.e., ARDIS® a joint venture between Motorola, Inc, and IBM) or a personal communication system (PCS) which is connected to the PSTN through a Mobile Network Integration (MNI) protocol without departing from the scope and spirit of the present invention.

Referring now to FIG. **2**, a flow chart of a preferred embodiment "point-to-point" encryption scheme used by the first **100** and the second **102** subscriber unit over the infrastructure **104**, **106**, and **108** is shown. One of the most important elements of this preferred embodiment encryption scheme is the encryption key management in a "point-to-point" communication system. As is described in USDC

system, each subscriber unit establishes a series of RF link encryption keys (e.g., SSD_A and SSD_B keys) upon registration with a cellular infrastructure network. These encryption keys, which are known to the subscriber unit and the cellular infrastructure network, are also known as registration keys. In addition as proposed by Brown et al., another encryption key, termed an SSD_C key, may be generated by each subscriber unit for use in data encryption. This SSD_C may also generate a session encryption key (SEK) which is valid for use during only one synchronous data communication session or one packet data registration session. The session encryption key (SEK) may be used to encrypt a "point-to-point" communication between the first **100** and the second **102** subscriber units such that the communication may even be encrypted as it passes through the infrastructure switch **104**.

The overall security of a communication channel between the first **100** and the second **102** subscriber units depends upon the secure passing of a session key to both subscriber units. Flowchart elements **200** through **218** outline a preferred embodiment technique for securely passing these session encryption keys. A first subscriber unit **100** makes **202** a request to the infrastructure communication center **104** for a secure communication link with a second subscriber unit **102** via the RF link **110**, first base site **106** and wireline **114**. This request preferably includes a session encryption key (SEK) which has been encrypted with a first subscriber registration key ($SSD1_C$). The infrastructure communication center **104** decrypts **204** the encrypted session encryption key (SEK) with the first subscriber registration key ($SSD1_C$). Subsequently, the infrastructure communication center re-encrypts **206** the session encryption key (SEK) with a second subscriber registration key ($SSD2_C$). At this point the infrastructure communication center **104** no longer needs the decrypted session encryption key and may optionally delete **208** the session key from an infrastructure memory device which temporarily stored the session key. This deleting of the decrypted session key may enhance the overall security of the communication system by eliminating the possibility that someone could get unauthorized access to the session keys by tapping into the infrastructure communication center **104** storage memory. The infrastructure communication center **104** then sends **210** the encrypted session encryption key (SEK) to the second subscriber unit **102** via

wireline **116**, second base site **108** and RF link **112**. The second subscriber unit **102** decrypts **212** the encrypted session encryption key (SEK) with the second subscriber registration key ($SSD2_C$). Finally, a message encrypted by the session encryption key (SEK) is communicated **214** between the first subscriber unit **100** and the second subscriber unit **102** transparently (i.e., without the decryption by the infrastructure) through the infrastructure communication center **104**. This message may be decrypted by either subscriber unit **100** or **102** with the session encryption key (SEK).

This method of session key (SEK) management also works for broadcast messaging systems wherein the encrypted session key (SEK) may be sent in step **210** to a plurality of second subscriber units **102** such that broadcast messages may be encrypted by the session key (SEK).

In addition, an encrypted conference communication link may be enabled **216** by the infrastructure communication center **104** through one of two methods. This type of conference communication link is also known as a fractional-duplex mode of encrypted speech for conference applications. The first subscriber unit **100** would broadcast the session key (SEK) to the other parties in the conference call. Then once the session key (SEK) is established, a conversation can proceed whereby each talker can speak individually to all of the others. A smooth conversation flow requires that either an agreement exist between all participants concerning the order of the talkers (which is common on amateur radio nets), or that an automatic speech detector select the "talker" and route the "talker's" encrypted speech to the other subscriber units. Automatic speech detection and directional routing are common in speakerphone devices for conversations between two endpoints; however, through sophisticated automatic routers at infrastructure communication centers **104** it is possible to handle three or more endpoints at a time. One method for enabling automatic routing by the infrastructure communication center **104** involves decrypting subsequent communications from all of the subscriber units in the conference communication link with the decrypted session encryption key (SEK) which was previously stored in the memory of the infrastructure communication center **104**. Another method for enabling automatic routing by the infrastructure communication center **104**

involves participating subscriber units **100** and **102** providing communication activity information to the infrastructure communication center **104**.

Referring now to FIG. **3**, a flow chart of an alternative preferred embodiment "point-to-point" encryption scheme used by the first **100** and the second **102** subscriber unit over the infrastructure **104**, **106**, and **108** is shown. Flowchart elements **300** through **318** outline the alternative preferred embodiment technique for securely passing these session encryption keys. In this alternative preferred embodiment, the first subscriber unit **100** and the infrastructure communication center **104** a priori know (i.e., have previously determined) the value of the session key (SEK) through the subscriber unit registration process or some other way. Therefore, the first subscriber unit **100** makes **302** a request, without including the session encryption key (SEK), to the infrastructure communication center **104** for a secure communication link with a second subscriber unit **102** via the RF link **110**, first base site **106** and wireline **114**. Subsequently, the infrastructure communication center encrypts **306** the session encryption key (SEK) with a second subscriber registration key ($SSD2_C$). At this point the infrastructure communication center **104** no longer needs the decrypted session encryption key and may optionally delete **308** the session key from an infrastructure memory device which temporarily stored the session key. The infrastructure communication center **104** then sends **310** the encrypted session encryption key (SEK) to the second subscriber unit **102** via wireline **116**, second base site **108** and RF link **112**. The second subscriber unit **102** decrypts **312** the encrypted session encryption key (SEK) with the second subscriber registration key ($SSD2_C$). Finally, a message encrypted by the session encryption key (SEK) is communicated **314** between the first subscriber unit **100** and the second subscriber unit **102** transparently (i.e., without the decryption by the infrastructure) through the infrastructure communication center **104**. This message may be decrypted by either subscriber unit **100** or **102** with the session encryption key (SEK). It will be appreciated by those skilled in the art that an encrypted conference communication link may be enabled **316** for this alternative preferred embodiment encryption scheme in a manner similar to the one

previously described in reference to the preferred embodiment encryption scheme shown in FIG. 2.

Although the invention has been described and illustrated with a certain degree of particularity, it is understood that the present disclosure of embodiments has been made by way of example only and that numerous changes in the arrangement and combination of parts as well as steps may be resorted to by those skilled in the art without departing from the spirit and scope of the invention as claimed. For example, the communication channel could alternatively be an electronic data bus, wireline, optical fiber link, satellite link, or any other type of communication channel.

Claims

What is claimed is:

1. A method of secure key distribution in a communication system having a plurality of subscriber units and an infrastructure communication center, comprising:
   (a) requesting, by a first subscriber unit to the infrastructure communication center, a secure communication link with a second subscriber unit, the request including an encrypted session encryption key, the session encryption key being encrypted with a first subscriber registration key;
   (b) decrypting, by the infrastructure communication center, the encrypted session encryption key with the first subscriber registration key;
   (c) re-encrypting, by the infrastructure communication center, the session encryption key with a second subscriber registration key; and
   (d) sending the encrypted session encryption key to the second subscriber unit.

2. The method of claim 1 further comprising the step of communicating a message encrypted by the session encryption key from the first subscriber unit to the second subscriber unit transparently through the infrastructure communication center.

3. The method of claim 1 further comprising the step of decrypting, by the second subscriber unit, the encrypted session encryption key with the second subscriber registration key.

4. The method of claim 1 wherein the sending step comprises sending the encrypted session encryption key to a plurality of second subscriber units.

5. The method of claim 1 further comprising the step of deleting, by the infrastructure communication center, the decrypted session encryption key from a memory device.

6. The method of claim 1 further comprising the step of enabling an encrypted conference communication link, by the infrastructure communication center, through decrypting subsequent communications from subscriber units with the decrypted session encryption key.

7. The method of claim 1 further comprising the step of enabling an encrypted conference communication link, by participating subscriber units, through providing communication activity information to the infrastructure communication center.

8. The method of claim 1 wherein in the step of requesting, the first subscriber unit and the infrastructure communication center know a priori the session encryption key.

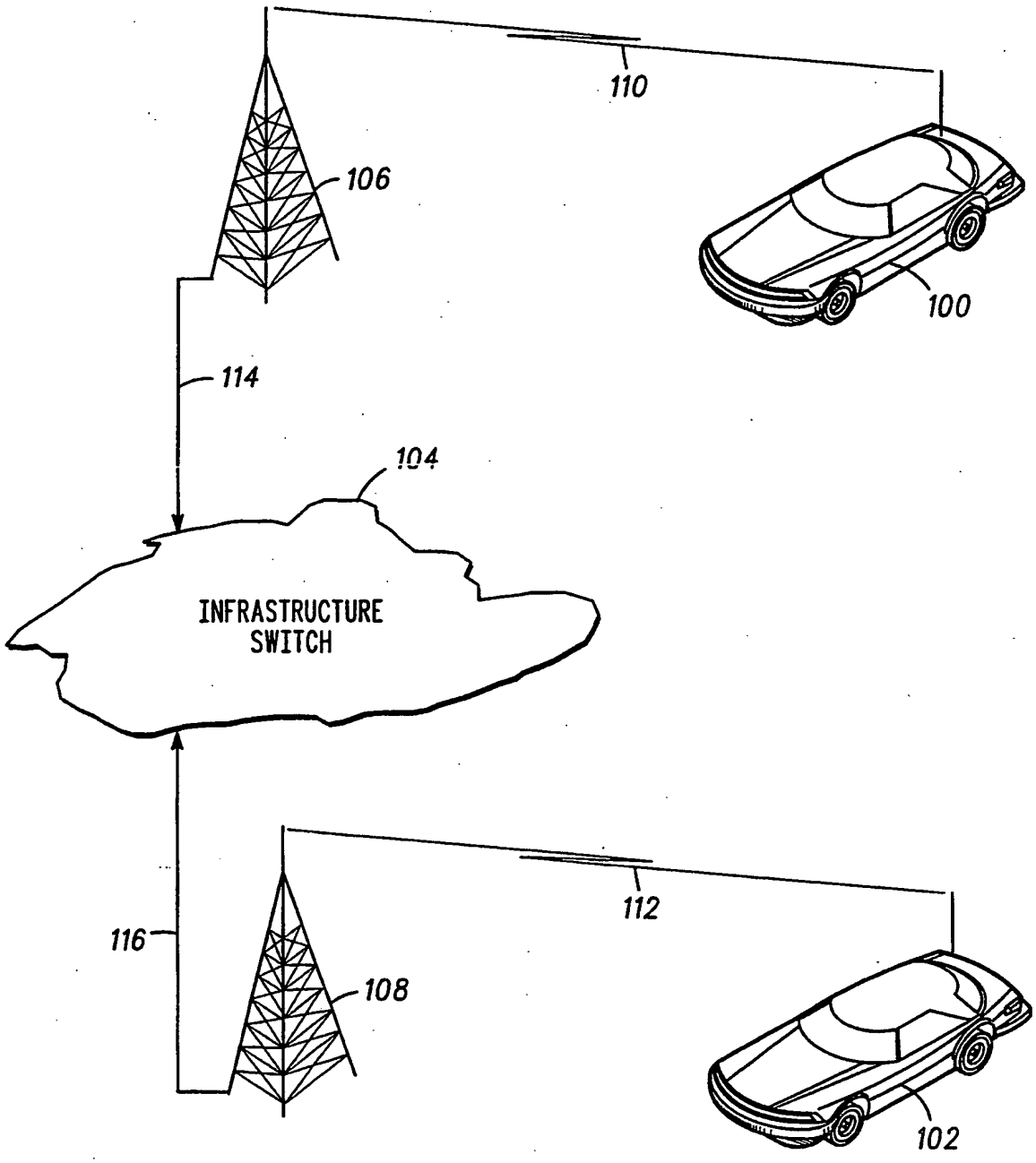


FIG.1

FIG. 2

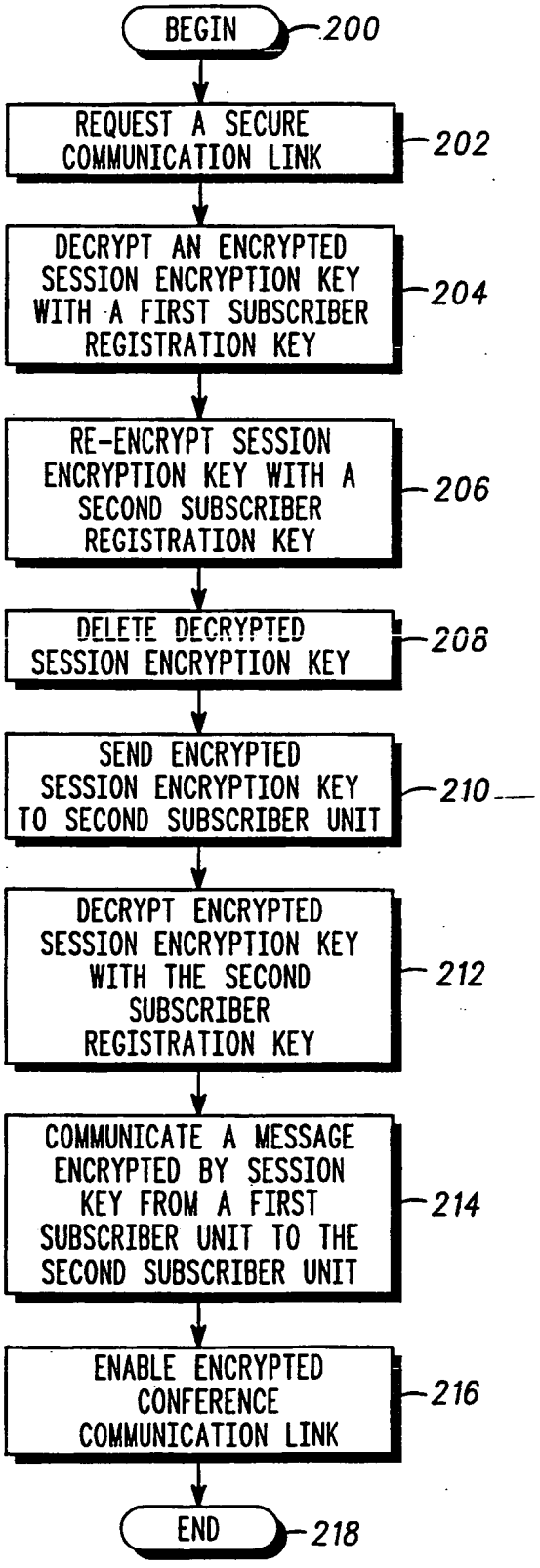
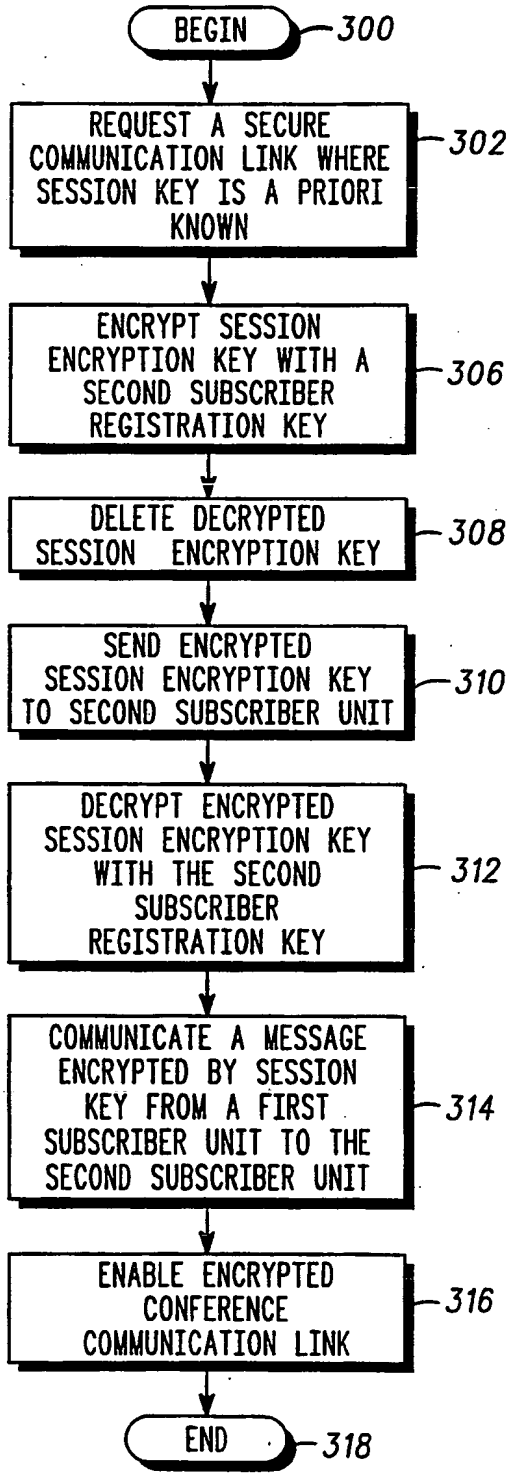

BEGIN
200
REQUEST A SECURE COMMUNICATION LINK
202
DECRYPT AN ENCRYPTED SESSION ENCRYPTION KEY WITH A FIRST SUBSCRIBER REGISTRATION KEY
204
RE-ENCRYPT SESSION ENCRYPTION KEY WITH A SECOND SUBSCRIBER REGISTRATION KEY
206
DELETE DECRYPTED SESSION ENCRYPTION KEY
208
SEND ENCRYPTED SESSION ENCRYPTION KEY TO SECOND SUBSCRIBER UNIT
210
DECRYPT ENCRYPTED SESSION ENCRYPTION KEY WITH THE SECOND SUBSCRIBER REGISTRATION KEY
212
COMMUNICATE A MESSAGE ENCRYPTED BY SESSION KEY FROM A FIRST SUBSCRIBER UNIT TO THE SECOND SUBSCRIBER UNIT
214
ENABLE ENCRYPTED CONFERENCE COMMUNICATION LINK
216
END
218

FIG. 3


BEGIN
300
REQUEST A SECURE COMMUNICATION LINK WHERE SESSION KEY IS A PRIORI KNOWN
302
ENCRYPT SESSION ENCRYPTION KEY WITH A SECOND SUBSCRIBER REGISTRATION KEY
306
DELETE DECRYPTED SESSION ENCRYPTION KEY
308
SEND ENCRYPTED SESSION ENCRYPTION KEY TO SECOND SUBSCRIBER UNIT
310
DECRYPT ENCRYPTED SESSION ENCRYPTION KEY WITH THE SECOND SUBSCRIBER REGISTRATION KEY
312
COMMUNICATE A MESSAGE ENCRYPTED BY SESSION KEY FROM A FIRST SUBSCRIBER UNIT TO THE SECOND SUBSCRIBER UNIT
314
ENABLE ENCRYPTED CONFERENCE COMMUNICATION LINK
316
END
318

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/09519

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :380/21, 43
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : Please See Extra Sheet.

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 5,124,117 (TATEBAYASHI, ET AL.) 23 June 1992	1-8

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 10 DECEMBER 1994	Date of mailing of the international search report 17 JAN 1995
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer DAVID CAIN Telephone No. (703) 308-0463

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/09519

B. FIELDS SEARCHED
Minimum documentation searched
Classification System: U.S.

380/21, 43,30,49

第 7 部門第 3 区分

全 8 頁

(19)日本国特許庁（ＪＰ）

(12) **公表特許公報（Ａ）**

(11)特許出願公表番号

特表平8－504073

(43)公表日 平成８年(1996)４月30日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	
Ｈ０４Ｌ 9/00				
Ｇ０９Ｃ 1/00		7259－5Ｊ		
Ｈ０４Ｌ 9/10				
		8842－5Ｊ	Ｈ０４Ｌ 9／00	Ｚ
		7605－5Ｊ	Ｈ０４Ｂ 7／26	１０９ Ｒ

審査請求 未請求 予備審査請求 未請求(全 18 頁) 最終頁に続く

(21)出願番号 特願平7－510303

(86) (22)出願日 平成６年(1994)８月25日

(85)翻訳文提出日 平成７年(1995)５月26日

(86)国際出願番号 ＰＣＴ／ＵＳ９４／０９５１９

(87)国際公開番号 ＷＯ９５／０９４９８

(87)国際公開日 平成７年(1995)４月６日

(31)優先権主張番号 ０８／１２７，７１８

(32)優先日 1993年９月27日

(33)優先権主張国 米国（ＵＳ）

(81)指定国 ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＦＩ，ＪＰ

(71)出願人 モトローラ・インコーポレイテッド
アメリカ合衆国イリノイ州60196シャンバーグ、イースト・アルゴンクイン・ロード1303

(72)発明者 フィンケルシュタイン，ルイス・ディビッド
アメリカ合衆国イリノイ州ウィーリング、ウェスト・オットワ・コート1698

(72)発明者 ブラウン，ダニエル・ピーター
アメリカ合衆国イリノイ州エルムハースト、チャタム・アベニュー788

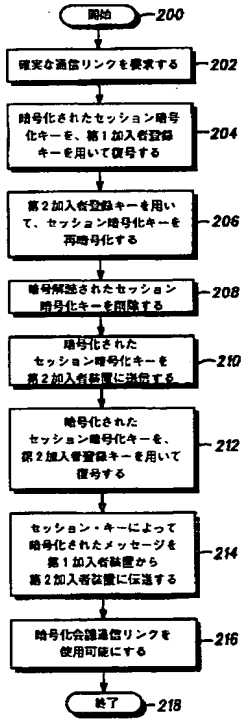
(74)代理人 弁理士 本城 雅則 (外１名)

最終頁に続く

(54)【発明の名称】 ポイント・ツー・ポイント通信のキー管理方法

(57)【要約】

複数の加入者装置１００，１０２およびインフラストラクチャ通信センタ１０４を有する通信システムにおける確実なキー分配の方法を提供する。第１加入者装置１００は、インフラストラクチャ通信センタ１０４に、第２加入者装置１０２との確実な通信リンクを求める要求を送信する２０２。この要求は、第１加入者登録キーを用いて暗号化された暗号化セッション暗号化キーを含む。インフラストラクチャ通信センタは、第１加入者登録キーを用いて、暗号化セッション暗号化キーを暗号解読する２０４。次にインフラストラクチャ通信センタは、第２加入者登録キーを用いて、セッション暗号化キーを再暗号化する２０６。この再暗号化セッシヨン暗号化キーは第２加入者装置に送信される２１０。



【特許請求の範囲】

１．複数の加入者装置およびインフラストラクチャ通信センタを有する通信システムにおける確実なキー分配の方法であって：

（ａ）第１加入者装置からインフラストラクチャ通信センタに、暗号化されたセッション暗号化キーを含む要求を送信する要求段階であって、前記セッション暗号化キーが第１加入者登録キーを用いて暗号化された前記要求段階；

（ｂ）インフラストラクチャ通信センタが、暗号化されたセッション暗号化キーを、第１加入者登録キーを用いて暗号解読する段階；

（ｄ）インフラストラクチャ通信センタが、第２加入者登録キーを用いてセッション暗号化キーを再暗号化する段階；および

（ｅ）暗号化されたセッション暗号化キーを第２加入者装置に送信する段階；

によって構成されることを特徴とする確実なキー分配の方法。

２．前記セッション暗号化キーによって暗号化されたメッセージを、インフラストラクチャ通信センタを介して前記第１加入者装置から前記第２加入者装置へ伝達する段階によってさらに構成されることを特徴とする請求項１記載の方法。

３．前記第２加入者装置が前記暗号化されたセッション暗号化キーを、前記第２加入者登録キーを用いて暗号解読する段階によってさらに構成されることを特徴とする請求項１記載の方法。

４．前記送信段階が前記暗号化されたセッション暗号化キーを複数の第２加入者装置に送信することから成ることを特徴とする請求項１記載の方法。

５．前記インフラストラクチャ通信センタが前記暗号解読されたセッション暗号化キーを記憶装置から削除することによってさらに構成されることを特徴とする請求項１記載の方法。

６．前記インフラストラクチャ通信センタが前記暗号解読されたセッション暗号化キーを用いて加入者装置からのその後の通信を暗号解読することにより、暗号化会議通信リンクを使用可能にする段階によってさらに構成されることを特徴とする請求項１記載の方法。

７．参加加入者装置が前記インフラストラクチャ通信センタへ通信活動情報を提供することにより、暗号化会議通信リンクを使用可能にする段階によってさらに構成されることを特徴とする請求項１記載の方法。

８．前記要求段階で、前記第１加入者装置および前記インフラストラクチャ通信センタが前記セッション暗号化キーセッション・キーを既知であることを特徴とする請求項１記載の方法。

【発明の詳細な説明】

ポイント・ツー・ポイント通信のキー管理方法

発明の分野

本発明は、通信システムに関し、さらに詳しくは、ポイント・ツー・ポイント通信の暗号化キー管理（encryptionkey management）に関する。

発明の背景

本発明は、本発明の譲受人に譲渡された次の発明に関連する。１９９３年６月２８日出願の米国特許出願番号第０８／０８４，６４４号が付与されたブラウンらによる”Method and Apparatus for Efficient Real-Time Authentication and Encryption in a Communication System”。

多くの通信システムは現在、システムのセキュリテイ（機密性）を向上するために、暗号化を使用する。そうした通信システムには、有線および無線データ網ばかりでなく、セルラ無線電話通信システム，パーソナル通信システム，ページング・システムも含まれる。以下では、例としてセルラ通信システムについて記述するが、ここで記述す

る暗号化技術は、本発明の範囲および精神から逸脱することなく、他の通信システムにも容易に敷衍できることを、当業者は理解されたい。ここでセルラ通信システムについて考えると、このシステムは一般に、無線周波数（ＲＦ）通信リンクを介して固定網通信装置（fixed network communication unit）と通信する加入者装置（移動機や携帯機等）を含む。典型的なセルラ通信システムは、少なくとも一つの基地局（つまり、通信装置）および交換局（switching center）（つまり、インフラストラクチャ通信センタ）を含む。現在のセルラ通信システムは、ＲＦ通信リンクを傍受した他人が通信を聞くことができない（例えば、音声会話を盗聴できない）ように、加入者装置と基地局装置との間のＲＦリンクで、両方の装置に知られた暗号化キーを使用することにより、通信を暗号化するように設計される。

一つのそうしたＲＦリンク暗号化技術が、米国ディジタル・セルラ（ＵＳＤＣ）標準（ＩＳ－５４およびＩＳ－５５として知られる）に規定され、ワシントンＤ．Ｃ．２０００６Ｎ．Ｗ．アイ・ストリート２００１番地の電子工業会（ＥＩＡ）によって発表される。ＵＳＤＣシステムの暗号化技術は、加入者装置と基地局通信装置との間で受け渡されて初めて、セッション暗号化キーを両方の装置に知らせることができる一連の専用メッセージを利用するものである。この暗号化キーは、ＵＳＤＣシステムにおける共通

秘密データ（ＳＳＤ：shared secret data）に基づく。認証プロセスには、SSD_Aキーが使用される。同様に、音声プライバシ機能には、SSD_Bキーが使用される。音声プライバシ機能の場合、初期伝送加入者メッセージに認証応答が含まれるが、その他のデータは暗号化されない。暗号化プロセスを開始するコマンドは、加入者にトラヒック・チャネルが割り当てられた後で、サービス提供者（つまり、基地局通信装置）から加入者に送られる。さらに、現在のシステム・アーキテクチャの設計は、音声だけでなくデータをも暗号化することに重点が置かれる。理想的には、データ通信の各セッションごとに暗号化キーを提供しなければならない。同期データ環境では、セッション・キーは、１回の（例えば、回線交換方式）データ通信（つまり「呼」）の持続時間中に使用される暗号化キーである。同様に、データ・パケット環境では、セッション・キーは、通信装置がサービス提供システムに登録したときから通信装置が次回に再登録するときまで使用される暗号化キーである。また、先に引用した１９９３年６月２８日出願の米国特許出願番号第０８／０８４，６４４号が付与されたブラウンらによる”Method and Apparatus for Efficient Real-Time Authentication and Encryption in a Communication System”と称する関連発明には、SSD_Cキーと呼ばれデータ・パケット暗号化に使用される別の暗号化キーがＵＳＤＣシステムに提案される。これらの通

信システムでは、パケット化データも暗号化する必要がある。パケット化データは、一般的な暗号化プロセスに別の問題を追加する。これは、データのパケットが通信ユニットと異なる時間に加入者装置に到達することができるためである（つまり、パケット・メッセージは「コネクションレス（connectionless）」であ

る）。これらのパケットは、暗号化されたのと同じ順序で再組立し暗号解読する必要がある。また、暗号化キーは、加入者が登録を行なうときにじか交渉することができない。したがって、パケット化データに関連するこれらの問題を緩和できる暗号化技術の必要性が存在する。

しかし、これまでに知られるこれらの暗号化技術は、通信チャネルに内在する盗聴のおそれに対する脆弱性の全てを取り扱うものではない。盗聴は、加入者装置と端点目的通信装置（endpoint target communication device）との間の通信チャネルにおける他の場所でも、例えば陸上回線電話のワイヤタッピング（wire tapping）などにより、依然発生し得る。加入者装置と端点目的通信装置との間のこうした通信は、「ポイント・ツー・ポイント」通信と呼ばれる。通信は、加入者装置と目的装置との間の通信リンクを介して最終的に結合されるまでに、幾つかの異なる物理的通信リンクに沿って伝わることがある。例えば、セルラ環境では、加入者装置の使用者が、事業所に配置された目的通信装置に対し、音声呼を発信することがある。その

呼を完了するには、基地局通信装置までのＲＦリンクに通信チャネルが設定されなければならない。さらに、この通信チャネルを、公衆電話交換網（ＰＳＴＮ）を介して事業所まで延長しなければならない。この事業所は、ＰＳＴＮに接続された専用電話網を有するかもしれない。その結果、最終的に目的通信装置と接続するためには、通信チャネルを専用網（private network）を介しても延長する必要があるかもしれない。現在、暗号化技術は、通信チャネル全体の中の個々の構成要素にしか適用されない（例えば、ＵＳＤＣシステムのＲＦリンクは暗号化できる）。しかし、ＰＳＴＮまたは専用網など他の構成要素は、ワイヤタッピングを介する盗聴に対し脆弱なままである。したがって、通信チャネルの他の場所における盗聴に関連するこうした問題を緩和できる暗号化技術の必要性も存在する。

発明の概要

これらの必要性およびその他は、複数の加入者装置およびインフラストラクチャ通信センタを有する通信システムにおける確実なキー分配（secure key distr

を概略的に示す。以下の例では、加入者装置１００、１０２は、同一インフラストラクチャ交換局１０４によってサービスを提供される。第１加入者装置１００は、ＲＦリンク１１０によって第１基地局１０６への通信チャネルを形成する。同様に、第２加入者装置１０２は、ＲＦリンク１１２によって第２基地局１０８への通信チャネルを形成する。また、第１基地局１０６および第２基地局１０８は、それぞれ有線１１４、１１６によってインフラストラクチャ交換局１０４への通信チャネルを形成する。

しかし、複数の交換局（例えば、セルラ交換局、市内ＰＳＴＮ交換局、および／または長距離キャリア交換局）を使用して、二つの加入者装置を接続することもできることを、当業者は理解されたい。また、二つの加入者装置は二つの異なるセルラ・システムの一部分であってもよく、あるいは一つが有線に接続され、一つがセルラ・システムの一部分であってもよい。さらに、加入者装置は、本発明の

範囲および精神から逸脱することなく、Advanced Radio Data Information Service（つまり、モトローラ社とＩＢＭの合弁企業であるＡＲＤＩＳ®）または、移動網統合（ＭＮＩ：Mobile Network Integration）プロトコルを用いてＰＳＴＮに接続されるパーソナル通信システム（ＰＣＳ）などの通信チャネルを介して、音声ではなくデータを通信することもできる。

次に第２図を参照して、インフラストラクチャ１０４、１０６、１０８を介して第１（１００）および第２（１０２）加入者装置によって使用される好適な実施例の「ポイント・ツー・ポイント」暗号化方式の流れ図である。この好適な実施例の暗号化方式で最も重要な要素の一つは、「ポイント・ツー・ポイント」通信システムにおける暗号化キー管理である。ＵＳＤＣシステムに規定されるように、各加入者装置は、セルラ・インフラストラクチャ網への登録直後に、一連のＲＦリンク暗号化キー（例えば、SSD_AおよびSSD_Bキー）を設定する。加入者装置およびセルラ・インフラストラクチャ網に知られるこれらの暗号化キーは、登録キーとも呼ばれる。さらに、ブラウンらによって提唱されたように、ＳＳ

ibution）の方法を提供することによって、実質的に満たされる。第１加入者装置は、インフラストラクチャ通信センタに対し、第２加入者装置との安全通信リンクの要求を送信する。この要求は、第１加入者登録キーを用いて暗号化された暗

号化セッション暗号化キー（encrypted session encryption key）を含む。インフラストラクチャ通信センタは、第１加入者登録キーを用いてこの暗号化セッション暗号化キーを暗号解読する。次に、インフラストラクチャ通信センタは、第２加入者登録キーを用いてセッション暗号化キーを再暗号化する。この再暗号化セッション暗号化キーは、第２加入者装置に送信される。別の方法では、第１加入者装置およびインフラストラクチャ通信センタが、セッション・キーを既知である。したがって、インフラストラクチャ通信センタは、第１加入者装置の要求に応答して、セッション暗号化キーを暗号化して第２加入者装置に送信するだけでよい。

図面の簡単な説明

第１図は、本発明に従って第１および第２加入者装置ならびにこれらの加入者装置を接続するインフラストラクチャを含む、好適な実施例の通信システムを示すブロック図である。

第２図は、本発明に従って第１図に示すインフラストラクチャを介して第１および第２加入者装置によって使用される、好適な実施例の暗号化方法の流れ図である。

第３図は、本発明に従って第１図に示すインフラストラクチャを介して第１および第２加入者装置によって使用さ

れる別の好適な実施例の暗号化方法の流れ図である。

詳細な説明

第１図は、第１（１００）および第２（１０２）加入者通信装置（例えば、無線電話），インフラストラクチャ通信センタまたは交換局などのインフラストラクチャ１０４，ならびに第１（１０６）および第２（１０８）セルラ無線基地局

D_Cキーと呼ばれる別の暗号化キーを、各加入者装置によってデータ暗号化用として生成することもできる。このSSD_Cは、１回の同期データ通信セッションまたは１回のパケット・データ登録セッションの間だけ有効に使用できるセッション暗号化キー（ＳＥＫ）を生成

することもできる。セッション暗号化キー（ＳＥＫ）は、それがインフラストラクチャ交換局１０４を介してもまだ通信を暗号化できるように、第１（１００）および第２（１０２）加入者装置間の「ポイント・ツー・ポイント」通信を暗号化するために使用することができる。

第１（１００）および第２（１０２）加入者装置間の通信チャネルの全体的なセキュリティは、両方の加入者装置へのセッション・キーの確実な受渡しに依存する。流れ図の２００から２１８までの要素は、これらのセッション暗号化キーを確実に受け渡す技術の好適な実施例を概説する。第１加入者装置１００は、ＲＦリンク１１０、第１基地局１０６、および有線１１４を介する第２加入者装置１０２との確実な通信リンクを、インフラストラクチャ通信センタ１０４に要求する２０２。この要求は、第１加入者登録キー（$SSD1_C$）を用いて暗号化されたセッション暗号化キー（ＳＥＫ）を望ましくは含む。インフラストラクチャ通信センタ１０４は、第１加入者登録キー（$SSD1_C$）を用いて、暗号化されたセッション暗号化キー（ＳＥＫ）を暗号解読する２０４。次に、インフラストラクチャ通信センタは、第２加入者登録キー（$SSD2_C$）を用いて、セッション暗号化キー（ＳＥＫ）を再暗号化する２０６。この時点で、インフラストラクチャ通信センタ１０４は、暗号解読されたセッション暗号化キーをそれ以上必要としないので、セッションキーを一時的に格納するインフラスト

ラクチャ記憶装置からセッション・キーを任意選択的に削除することができる２０８。暗号解読されたセッション・キーをこのように削除すると、インフラストラクチャ通信センタ１０４の記憶装置へタッピングによって、誰かがセッション・キーに無許可アクセスを達成できる可能性が排除され、通信システムの全体的なセキュリティを向上することができる。次に、インフラストラクチャ通信セン

タ104は、暗号化されたセッション暗号化キー（SEK）を、有線116、第2基地局108、およびRFリンク112を介して第2加入者装置102へ送信する210。第2加入者装置102は、第2加入者登録キー（SSD2c）を用いて、暗号化されたセッション暗号化キー（SEK）を暗号解読する212。最後に、セッション暗号化キー（SEK）によって暗号化されたメッセージが、インフラストラクチャ通信センタ104を介して、第1加入者装置100と第2加入者装置102との間で透過的に（つまり、インフラストラクチャによる暗号解読を経ることなく）伝達される214。このメッセージは、セッション暗号化キー（SEK）を用いて、加入者装置100、102のどちらでも暗号解読することができる。

この方法によるセッション・キー（SEK）管理は、同報通信メッセージ・システム（broadcast messaging system）にも有効であり、セッション・キー（SEK）によって同報通信メッセージを暗号化できるように、ステッ

プ210で複数の第2加入者装置102に暗号化セッシヨン・キー（SEK）を送信することができる。

また、二通りの方法のうちの一つを用いて、インフラストラクチャ通信センタ104によって、暗号化会議通信リンクを使用可能にすることができる216。この種の会議通信リンクは、会議用の部分二重（fractional-duplex）モード暗号化通話としても知られる。第1加入者装置100が、会議電話の他の当事者にセッション・キー（SEK）を同報通信する。次に、いったんセッション・キー（SEK）が設定されると、会話を進めることができ、それによって各話者は他の全員と個々に通話することができる。円滑な会議の流れのためには、全参加者の間に話者の順番に関する合意が存在する（これは、アマチュア無線ネットで一般的である）か、または自動音声検出器が「話者」を選択し、「話者」の暗号化された音声を他の加入者装置に向けて経路選択することが必要になる。自動音声検出器および方向経路選択は、2端点間の会話用スピーカホン装置には一般的であるが、インフラストラクチャ通信センタ104における高度な自動ルータを用いて、三つ以上の端点を同時に処理することが可能である。インフラストラクチ

化されたセッション暗号化キー（SEK）を暗号解読する312。最後に、セッション暗号化キー（SEK）によって暗号化されたメッセージが、第1加入者装置100と第2加入者装置102との間でインフラストラクチャ通信センタ104を介して透過的に（つまり、インフラストラクチャによる暗号解読を経ることなく）伝達される314。このメッセージは、セッション暗号化キー（SEK）を用いて、加入者装置100、102のどちらでも暗号解読することができる。この別の好適な実施例の暗号化方式の場合、第2図に示す好適な実施例の暗号化方式に関連して先に説明したのと同様の方法で、暗号化会議通信リンクを使用可能にすることができる316ということを、当業者は理解されたい。

以上、本発明をある程度特定的に説明し図解したが、実施例のこの開示は例として行なったものにすぎず、当業者は、請求項に記載する本発明の精神および範囲から逸脱す

ることなく、方法だけでなく部品の配列や組合せについても様々な変化を思いつくことができることが理解される。例えば、通信チャネルは代替的に電子データ・バス、有線、光ファイバ・リンク、衛星リンク、またはその他の種類の通信チャネルとすることができる。

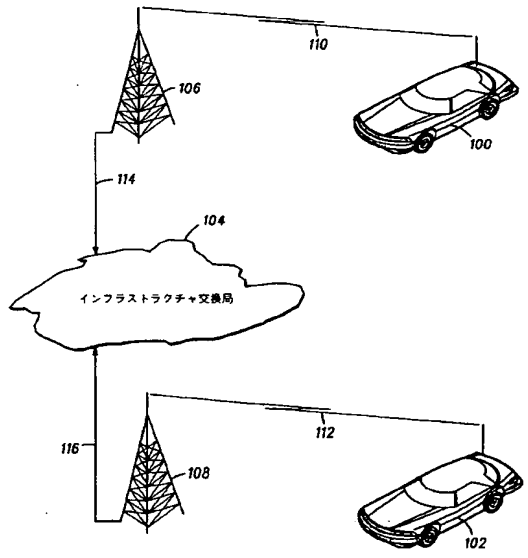
ャ通信センタ104によって自動経路指定を可能にする一つの方法は、会議通信リンク内の全ての加入者装置からのその後の通信を、インフラストラクチャ通信センタ104の記憶装置に予め格納された暗号解読されたセッション暗号

化キー（SEK）を用いて暗号解読することを含む。インフラストラクチャ通信センタ104によって自動経路選択を可能にする別の方法は、参加加入者装置100、102からインフラストラクチャ通信センタ104に通信活動情報を提供することを含む。

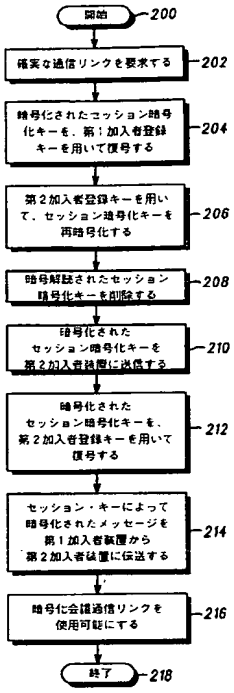
次に、第3図を参照して、これは、インフラストラクチャ104、106、108を介して、第1（100）および第2（102）加入者装置によって使用される別の好適な実施例の「ポイント・ツー・ポイント」暗号化方式の流れ図である。300から318までの流れ図の要素は、これらのセッション暗号化キーを確実に受け渡す技術の別の好適な実施例を概説する。この別の好適な実施例では、第1加入者装置100およびインフラストラクチャ通信センタ104は、加入者装置登録プロセスまたはその他の何らかの方法により、セッション・キー（SEK）の値は既知である（つまり、予め決められる）。したがって、第1加入者装置100は、RFリンク110、第1基地局106、および有線114を介した第2加入者装置102との確実な通信リンクを、インフラストラクチャ通信センタ104に、セッション暗号化キー（SEK）を用いずに要求する302。次に、インフラストラクチャ通信センタは、第2加入者登録キー（SSD2c）を用いて、セッション暗号化キー（SEK）を暗号化する306。この時点で、インフラストラクチャ通信センタ104は、暗号読解された

セッション暗号化キーをそれ以上必要としないので、セッション・キーを一時的に格納するインフラストラクチャ記憶装置からセッション・キーを任意選択的に削除することができる308。次に、インフラストラクチャ通信センタ104は、暗号化されたセッション暗号化キー（SEK）を、有線116、第2基地局108、およびRFリンク112を介して第2加入者装置102へ送信する310。第2加入者装置102は、第2加入者登録キー（SSD2c）を用いて、暗号

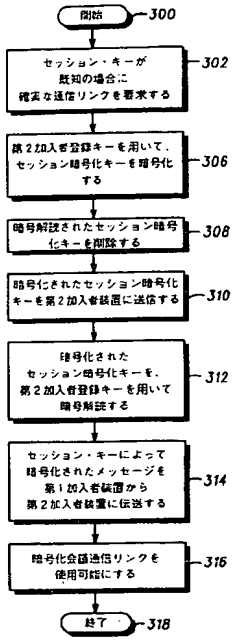
【図1】



【図2】


開始
200
確実な通信リンクを要求する
202
暗号化されたセッション暗号化キーを、第1加入者登録キーを用いて復号する
204
第2加入者登録キーを用いて、セッション暗号化キーを再暗号化する
206
暗号解読されたセッション暗号化キーを削除する
208
暗号化されたセッション暗号化キーを第2加入者装置に送信する
210
暗号化されたセッション暗号化キーを、第2加入者登録キーを用いて復号する
212
セッション・キーによって暗号化されたメッセージを第1加入者装置から第2加入者装置に伝送する
214
暗号化会議通信リンクを使用可能にする
216
終了
218

【図3】


開始
300
セッション・キーが既知の場合に確実な通信リンクを要求する
302
第2加入者登録キーを用いて、セッション暗号化キーを暗号化する
306
暗号解読されたセッション暗号化キーを削除する
308
暗号化されたセッション暗号化キーを第2加入者装置に送信する
310
暗号化されたセッション暗号化キーを、第2加入者登録キーを用いて暗号解読する
312
セッション・キーによって暗号化されたメッセージを第1加入者装置から第2加入者装置に伝送する
314
暗号化会議通信リンクを使用可能にする
316
終了
318

フロントページの続き

(51) Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ
Ｈ０４Ｌ	9/12		
Ｈ０４Ｑ	7/38		

(72)発明者　プール、ラリー・チャールズ
アメリカ合衆国イリノイ州スリーピィ・ホロウ、プラム・コート６

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/09519

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00
US CL :380/21, 43
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : Please See Extra Sheet.

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 5,124,117 (TATEBAYASHI, ET AL.) 23 June 1992	1-8

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
10 DECEMBER 1994	17 JAN 1995
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer DAVID CAIN Telephone No. (703) 308-0463

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/09519

B. FIELDS SEARCHED
Minimum documentation searched
Classification System: U.S.

380/21. 43.30.49